**19-letnia podatność w WinRAR. Pół miliarda użytkowników zagrożona.**

**WinRAR, popularny program do kompresji i archiwizacji danych z podatnością! Wykryty przez firmę Check Point exploit działa poprzez wyodrębnienie archiwum i naraża na niebezpieczeństwo ponad 500 milionów użytkowników! O dziwo, błąd ten istnieje od ponad 19 lat i zmusił WinRAR do całkowitego zarzucenia wsparcia dla podatnego na atak formatu.**

Kilka miesięcy temu zespół badawczy firmy Check Point zbudował wieloprocesorowe laboratorium fuzzingowe i rozpoczął „fuzz” plików binarnych środowisk Windows przy użyciu fuzzera WinAFL.

- *Po dobrych wynikach pozyskanych od Adobe Research zdecydowaliśmy się rozszerzyć nasze wysiłki związane z fuzzingiem i zaczęliśmy także fuzz WinRAR-a. –* pisze na blogu Nadav Grossman, ekspert Check Pointa odpowiedzialny za odkrycie podatności.

Jedna z awarii wywoływanych przez fuzzer zaprowadziła badaczy do starej biblioteki linków dynamicznych (DLL), która została skompilowana w 2006 roku bez mechanizmu ochrony (jak ASLR, DEP itp.) i która jest wciąż używana przez WinRAR.

**Zespoł zwrócił szczególną uwagę** na ten dll, a następnie próbował wyszukać błąd uszkodzenia pamięci, który mógł doprowadzić do zdalnego wykonania kodu. Jednak fuzzer w teście wykrył dziwne zachowanie. Po jego zbadaniu, ekipa Check Pointa wykryła błąd logiczny: Absolute Path Traversal. Od tego momentu łatwo było wykorzystać tę lukę do zdalnego wykonywania kodu.

WinRAR to narzędzie do archiwizacji plików dla systemu Windows, może tworzyć i wyświetlać archiwa w formatach plików RAR lub ZIP i rozpakowywać wiele innych formatów archiwalnych. Jak wskazuje strona internetowa WinRAR, "Ponad 500 milionów użytkowników na całym świecie sprawia, że WinRAR jest dziś najpopularniejszym na świecie narzędziem do kompresji".

Analiza techniczna podatności WinRAR dostępna jest na blogu firmy Check Point: <https://research.checkpoint.com/>